عنوان مقاله:
افزایش قابلیت های Snort برای هوشمند سازی سیستم تشخیص نفوذ

محل انتشار:
همایش دستاوردهای نوین در هوافضا و صنعت هواپیمایی ایران (سال: 1396)

تعداد صفحات اصل مقاله: 13

نویسنده:
سید محسن هاشمی - *دانشگاه آزاد اسلامی واحد بروجرد*

خلاصه مقاله:
محرمانگی ، تمامیت و در دسترس بودن ، نگرانی های اصلی در توسعه و استخراج سیستم های یارانه ای مبتنی بر شبکه است . عظمت فراساختارهایشبکه ای ، موجب افزایش آسیب پذیری این سیستم ها در قبال تهدیدهای امنیتی ، حملات و نفوذ هاست. ارتباط شبکه های مختلف با یکدیگر و تنوعاستفاده کنندگان سبب بروز مشکلات عمده ای نظیر سرقت ، تخریب و دستکاری اطلاعات شده است . بدین منظور سیستم هایی تحت عنوان سیستمهای تشخیص نفوذ به منظور شناسایی رفتارهای مشکوک به وجود آمده اند به طوریکه امروزه در شبکه های کامپیوتری از این سیستم ها به عنوان یکابزار تدافعی در برابر حملات و به منظور حفاظت از اطلاعات استفاده می کنند. در این پایان نامه ، رویکردی جدید نسبت به توسعه سیستم های تشخیص نفوذ هوشمند برای تشخیص حملات معرفی می شود . به این صورت که ضمن بررسی روش ها و تکنیک های تشخیص نفوذ و بررسی سیستم های تشخیص نفوذ ، سیستم Snort را که به عنوان ابزاری مناسب ، بخش وسیعی از امنیت شبکه ها را به خود اختصاص داده است را انتخاب و با ارایه روشی مناسب مهمترین محدودیت این سیستم که عدم تشخیص رفتار غیر عادی و حمله های جدید است را برطرف می نماییم . روش ارایه شده به میزان قابل توجهی درصد نرخ تشخیص را افزایش می دهد و تا 20 درصد بهبود نسبت به وضعیت قبلی حاصل می شود. در این تحقیق از سیستم یادگیری

کلمات کلیدی:
, Intrusion Detection , Snort